Subrings of Algebraic Number Fields

By R. A. BEAUMONT and R. S. PIERCE[1]) in Seattle (Washington, U. S. A.)

1. Introduction. This paper is a continuation of the authors' work ([1] and [5]) on torsion-free rings. We are concerned here with subrings of algebraic number fields. Throughout the paper, K will denote a fixed algebraic number field and J will denote the ring of algebraic integers in K. We will restrict our attention to subrings of K whose quotient field is all of K. Since K can be arbitrary, this is not really and additional restriction. If A is any subring of K, then QA (where Q is the field of rational numbers) is a subfield of K. Thus if the quotient field of A is K, then A is *full* in K in the sense that for any $x \in K$, there is a non-zero integer n such that $nx \in A$.

The paper is mainly devoted to the problem of classifying the subrings of K. In the first section we classify the (full) subrings of K up to the equivalence relation quasi-equality. Two subrings A and B of K are called *quasi-equal* (symbolically, $A \doteq B$) if $A \cap B$ has finite index in both A and B. Because of the finiteness of rank, this is equivalent to the existence of a non-zero integer n such that $nA \subseteq B$ and $nB \subseteq A$. The basic result of Section 2 is that each quasi-equality class of full subrings of K contains a unique integrally closed ring which is the largest ring in the quasi-equality class. It follows that the various quasi-equality classes of subrings of K are in one-to-one correspondence with sets of prime ideals of J. In Section 3 we take up the classification of the rings belonging to a given quasi-equality class. The results of Section 2 make this equivalent to finding all subrings of finite index in an integrally closed subring of K. We show that if J_Π is the integrally closed subring of of K associated with the set Π of prime ideals of J, then there is a one-to-one correspondence between the subrings of finite index in J_Π and the open subrings of the compact topological ring $\sum_{P \in \Pi}^{*} J(P)$, where $J(P)$ is the P-adic completion of J with the metric topology and the product topology is imposed on the complete direct sum.

[1]) This work was supported by the National Science Foundation Research Grant NSF — G 11098.

Using this result, it is possible to characterize those sets Π such that J_Π contains no proper subring of finite index having an identity element. In Section 4, we characterize in strictly group theoretical terms those torsion free abelian groups which are isomorphic to the additive group of a subring of an algebraic number field.

Generally speaking, in this paper the notation and terminology of [1] and [5] is used. Exceptions are the use of Q to denote the field of rationals and $Z(p)$ and $Q(p)$ to denote the p-adic completions of Z (the ring of integers) and Q respectively. If P is any prime ideal of the ring J, let $J_P=\{x/y|x,\ y\in J,\ y\notin P\}$. Also, if Π is a set of prime ideals in J, define

$$J_\Pi=\bigcap_{P\in\Pi} J_P.$$

Note that $J_\emptyset=K$. Denote by v_P the valuation of K associated with the prime ideal P of J. It is not necessary to normalize v_P. Thus v_P can be defined on J by letting $v_P(0)=0$ and for $x\neq 0$, $v_P(x)=p^{-k}$, where p is the unique rational prime in P and P^k is the highest power of P dividing the principal ideal (x). Then v_P is extended multiplicatively to K. It is also convenient to extend v_P to the non-zero ideals of J, defining $v_P(I)=p^{-k}$, where P^k is the highest power of P dividing I. Then v_P satisfies the inequality

$$v_P(x-y)\leqq \max\{v_P(x), v_P(y)\},\quad x, y\in K,$$

and if $v_P(x)\neq v_P(y)$, then equality holds. Moreover, it is easy to show that for any $x\in K$, $v_P(x)\leqq 1$ if and only if $x\in J_P$. Denote by $J(P)$ and $K(P)$ the completions of J and K with respect to v_P. Then $J(P)$ and $K(P)$ are metric topological rings (containing J and K respectively) with a metric which extends v_P. The extended metric can be denoted by v_P without confusion. As a topological space, $J(P)$ is compact. It is well known that the identical mapping of J into $J(P)$ can be extended to an isomorphism Δ_P of J_P into $J(P)$. Note that $v_P(\Delta_P x)=v_P(x)$.

2. Classification of quasi-equality classes. The proof of the main theorem of this section is based on the results of [1]. To make this proof intelligible, it is necessary to explain some of the concepts introduced there. Define a ring q. d. invariant of K to be a function δ which assigns to each rational prime p an ideal δ_p in the ring $Q(p)\otimes K$. The ring q. d. invariants are ordered by defining $\delta\leqq\delta'$ if $\delta_p\subseteq\delta'_p$ for all p. With this ordering, the ring q. d. invariants form a complete lattice (actually, a complete, atomic Boolean algebra). There is also a natural way to order the quasi-equality classes of full subrings of K. This is obtained by defining the class of the ring A to be less than or equal to the class of the ring B if $nA\subseteq B$ for some non-zero integer n.

Lemma 2.1. *There is a one-to-one order preserving correspondence between the quasi-equality classes of full subrings of K and the ring q. d. invariants of K. This correspondence is induced by the mapping which associates with the full subring A the q. d. invariant $\delta(A)$, where $\delta_p(A)$ is the maximal divisible subgroup of $Z(p)\otimes A$ (considered as a subgroup of $Q(p)\otimes K$).*

Proof. See [1, Corollary 4.9 and Theorem 1.10].

It follows from this result alone that there is a one-to-one correspondence between the quasi-equality classes of full subrings of K and the subsets of the prime ideals of J. Indeed, it is a classical result (due essentially to Hensel) that

$$Q(p)\otimes K \cong K(P_1) \dotplus \cdots \dotplus K(P_g), \tag{1}$$

where $P_1, \ldots, P_g$ are the distinct prime ideal divisors of the principal ideal (p) (see [3, pp. 96—98]). The ideals of the ring $K(P_1) \dotplus \cdots \dotplus K(P_g)$ are precisely the partial sums $K(P_{i_1}) \dotplus \cdots \dotplus K(P_{i_r})$, where $1 \leqq i_1 < \cdots < i_r \leqq g$. Thus, the ring q. d. invariants can be determined by specifying the set $P_{i_1}, \ldots, P_{i_r}$ of prime ideals corresponding to each rational prime p. For future reference, we note that the projections $\pi_i : Q(p)\otimes K \to K(P_i)$ corresponding to the isomorphism (1) are obtained by mapping

$$\sum_{j=1}^{m}\left(\sum_{k=-n}^{\infty} a_{jk}p^k\right)\otimes x_j \to \sum_{k=-n}^{\infty}\left(\sum_{j=1}^{m} a_{jk}p^k x_j\right), \quad a_{jk}\in Z, \tag{2}$$

where the infinite sum on the left is taken in the p-adic topology of $Q(p)$ and the infinite sum on the right side is taken in the topology of the metric v_{P_i} on $K(P_i)$.

Our first objective in this section is to determine the q. d. invariants associated with the various rings J_P. It is convenient to obtain these indirectly.

If A is a subring of K, then we say that $x \in K$ is integral over A, if x is integral (in the usual sense) over the ring $\{A, 1\}$ where 1 is the identity of K. By the integral closure of A, we mean the ring of all elements of K which are integral over A. It is easy to show (see [4]) that the integral closure of A is the intersection of all valuation rings J_P containing A, since $J_P \supseteq A$ if and only if $J_P \supseteq \{A, 1\}$.

Lemma 2.2. *If A is a proper full subring of K, then $A \subseteq J_P$ for some proper prime ideal P of J.*

Proof. By the above remarks, it is sufficient to show that the integral closure of A is a proper subring of K. Since A is a full subring of K, there is an integer $n \neq 0$ such that $n\cdot 1 \in A$. Thus $\{A, 1\}/A$ has bounded order.

Since A is a proper subring of K, K/A is a non-trivial divisible group. Hence $\{A, 1\} \neq K$, that is, $\{A, 1\}$ is a proper subring of K. Thus, there is a rational prime p such that $1/p \notin \{A, 1\}$. Then $1/p$ is not integral over A, because $(1/p)^n + a_1(1/p)^{n-1} + \cdots + a_n = 0$, $a_i \in \{A, 1\}$ implies that $1/p = -(a_1 + \cdots + p^{n-1}a_n) \in \{A, 1\}$.

Lemma 2.3. *If A is a subring of K, P is a prime ideal of J, and if $nA \subseteq J_P$ for some non-zero integer n, then $A \subseteq J_P$.*

Proof. Let $x \in A$. Then $x^k \in A$ for all exponents $k \geqq 1$. Hence $v_P(n)v_P(x)^k = v_P(nx^k) \leqq 1$. Since k can be arbitrarily large, this implies that $v_P(x) \leqq 1$. Therefore $x \in J_P$.

Corollary 2.4. *If P is a prime ideal of J, then $\delta(J_P)$ is a maximal ring q. d. invariant.*

Proof. By Lemmas 2.2 and 2.3, and the fact that there are no inclusion relations between distinct valuation rings, the quasi-equality classes of the rings J_P are maximal. Hence, the corollary follows from Lemma 2.1.

Lemma 2.5. *Let P be a prime ideal of J. Let p be the rational prime belonging to P. Then if $q \neq p$, $\delta_q(J_P) = Q(q) \otimes K$. Under the isomorphism (1), $\delta_p(J_P)$ corresponds to $K(P_1) \dotplus \cdots \dotplus K(P_{i-1}) \dotplus K(P_{i+1}) \dotplus \cdots \dotplus K(P_g)$, where $P_i = P$.*

Proof. Since $\delta_p(J_P)$ is an ideal, $\pi_i(\delta_p(J_P)) = K(P_i)$ or 0. If $\pi_i(\delta_p(J_P)) = K(P_i)$, then $\pi_i(Z(p) \otimes J_P) = K(P_i)$. But this is impossible since $v_{P_i}(x) \leqq 1$ for all $x \in J_P = J_{P_i}$ and it follows readily from (2) that $v_{P_i}(z) \leqq 1$ for all $z \in \pi_i(Z(p) \otimes J_P)$. The lemma now follows from Corollary 2.4.

Lemma 2.6. *Let Π be a set of prime ideats of J. Then $\delta(J_\Pi) =$ = g. l. b. $\{\delta(J_P) | P \in \Pi\}$.*

Proof. Since $J_\Pi \subseteq J_P$ for all $P \in \Pi$, $\delta(J_\Pi) \leqq$ g. l. b. $\{\delta(J_P) | P \in \Pi\}$. By Lemma 2.1, there is a ring A such that $\delta(A) =$ g. l. b. $\{\delta(J_P) | P \in \Pi\}$. Thus $\delta(A) \leqq \delta(J_P)$ for all $P \in \Pi$. Hence, by Lemmas 2.1 and 2.3, $A \subseteq J_P$ for all $P \in \Pi$. Consequently, $A \subseteq \bigcap_{P \in \Pi} J_P = J_\Pi$. This implies that

$$\text{g. l. b. } \{\delta(J_P) | P \in \Pi\} = \delta(A) \leqq \delta(J_\Pi).$$

Theorem 2.7. *In each quasi-equality class of full subrings of K, there is one and only one integrally closed ring. This ring is the integral closure of every ring in the class.*

Proof. By Lemmas 2.5 and 2.6, $\delta_p(J_\Pi)$ is isomorphic to the ring direct sum of all $K(P)$ with $p \in P \in \Pi^c$. Thus, by Lemma 2.1, if $\Pi_1 \neq \Pi_2$,

then J_{Π_1} is not quasi-equal to J_{Π_2}, and every quasi-equality class contains one of the rings J_Π. Since J_Π is an intersection of valuation rings, it is integrally closed. Suppose $A \doteq J_\Pi$. If $P \in \Pi$, then $nA \subseteq J_P$ for some non-zero integer n. Thus, by Lemma 2.3, $A \subseteq J_P$. Consequently, $A \subseteq J_{\Pi'} \subseteq J_\Pi$, where $\Pi' = \{P | J_P \supseteq A\}$ and $J_{\Pi'}$ is the integral closure of A. This implies that $J_{\Pi'} \doteq J_\Pi$ and therefore $\Pi' = \Pi$.

Remarks. It follows from Theorem 2.7 that the conductor of the integral closure of any subring of an algebraic number field is a non-zero ideal. Thus it is possible to reduce a large part of the ideal theory of such a ring to that of its integral closure (see [4, pp. 91—92]). Moreover, if A is any full subring of K, then every non-zero ideal I of A contains a non-zero integer (since $0 \neq x \in I$ and $nx^{-1} \in A$ implies $n \in I$) and therefore A/I is a group of finite rank and bounded order. Thus, A/I must be finite. This observation has the consequences that A is Noetherian and its prime ideals are maximal. If A is also integrally closed, then it is a Dedekind ring. It is easy to see that the prime ideals of J_Π are precisely the ideals PJ_Π, where $P \in \Pi$.

Although the quasi-equality classes of full subrings of K are completely specified by designating a set of prime ideals of J, it is convenient for some purposes to label these classes in a different way.

Definition 2.8. Let Π be a set of prime ideals of J. For each rational prime p, let

$$I_p(\Pi) = P_1^{e_1} \dots P_k^{e_k},$$

where $P_1, \dots, P_k$ are the distinct prime ideals in Π which contain p, and e_i is the highest power of P_i dividing (p) (that is, e_i is the ramification index of P_i in (p)). If no prime ideal in Π contains p, let $I_p(\Pi) = J$.

If $\{I_p\}$ is a system of ideals of J (one for each rational prime p), then there is a set Π of prime ideals of J such that $I_p = I_p(\Pi)$ for all p if and only if for each p, $(p) = I_p I_p'$ with I_p and I_p' relatively prime. Moreover the set Π is uniquely determined as the set of all prime ideals P such that P divides one of the ideals I_p.

Proposition 2.9. *Let F be a subfield of K and denote by J_0 the ring of integers in F. Let Π_0 be a set of prime ideals of J_0 and define $\Pi = \{P$, prime ideal of $J | P \supseteq P_0$ for some $P_0 \in \Pi_0\}$. For any $P_0 \in \Pi_0$, let J_{0P_0} be the valuation ring of F associated with P_0 and let $J_{0\Pi_0} = \bigcap_{P_0 \in \Pi_0} J_{0P_0}$. Then*

(i) *J_Π is the integral closure of $J_{0\Pi_0}$ in K;*

(ii) *there is a basis $\{x_1, \dots, x_m\}$ of K over F such that*

$$J_\Pi \doteq J_{0\Pi_0} x_1 + \dots + J_{0\Pi_0} x_m;$$

(iii) $J_{0\Pi_0} = J_\Pi \cap F$;

(iv) $I_p(\Pi) = I_p(\Pi_0) \cdot J$ *for all* p.

Proof. By definition, J_Π is the intersection of all valuation rings of K which contain $J_{0\Pi_0}$. Thus, J_Π is the integral closure of $J_{0\Pi_0}$. To prove (ii), note that there is a basis $\{x_1, \ldots, x_m\}$ of K over F such that $J_\Pi \subseteq J_{0\Pi_0} x_1 + \cdots + J_{0\Pi_0} x_m$ (see [6, p. 264]). If n is a non-zero integer such that $n x_i \in J_\Pi$ for $i = 1, \ldots, m$, then $n(J_{0\Pi_0} x_1 + \cdots + J_{0\Pi_0} x_m) \subseteq J_\Pi$. Thus, these two groups are quasi-equal. The property (iii) follows from the observations that $J_\Pi \cap F \supseteq J_{0\Pi_0}$ and every element of $J_\Pi \cap F$ is integral over the integrally closed ring $J_{0\Pi_0}$. The statement (iv) is clear from the definitions of $I_p(\Pi)$ and $I_p(\Pi_0)$ because of the unique factorization of ideals in J.

The notion of *field of definition* of a subring of a simple algebra was introduced in [1] and [5]. For full subrings of K, this concept can be stated as follows: a field $F \subseteq K$ is a field of definition of A if $A \doteq (A \cap F) x_1 + \cdots + (A \cap F) x_m$ for some (or equivalently, any) basis $\{x_1, \ldots, x_m\}$ of K over F. It is easy to see that if two rings are quasi-equal, then they have the same fields of definition. Proposition 2.9 leads to a useful characterization of the fields of definition of the ring J_Π.

Theorem 2.10. *Let Π be a set of prime ideals of J. Then a field F in K is a field of definition of J_Π if and only if each of the ideals $I_p(\Pi)$ is generated by elements of F.*

Proof. Suppose that F is a field of definition of J_Π. Let J_0 be the ring of integers in F. Since $J_\Pi \cap F$ is integrally closed in F, there is a set Π_0 of prime ideals of J_0 such that $J_\Pi \cap F = J_{0\Pi_0}$. Since F is a field of definition of J_Π, it follows that $J_\Pi \doteq J_{0\Pi_0} x_1 + \cdots + J_{0\Pi_0} x_m$, where $\{x_1, \ldots, x_m\}$ is a basis of K over F. Then by Proposition 2.9, $J_\Pi \doteq J_{\Pi'}$, where Π' consists of all prime ideals of J which contain a prime ideal of Π_0. By Theorem 2.7, this implies that $\Pi' = \Pi$ and therefore by Proposition 2.9, $I_p(\Pi) = I_p(\Pi_0) J$. In particular, $I_p(\Pi)$ is generated by elements of F. Conversely, suppose that each $I_p(\Pi)$ is generated by elements of F. Let Π_0 be the totality of prime ideals of J_0 which divide some $I_p(\Pi) \cap F$. Let Π' be all prime ideals of J which contain some ideal of Π_0. If $P \in \Pi$, then $P_0 = P \cap F \supseteq I_p(\Pi) \cap F$ for some p. Hence $P_0 \in \Pi_0$ and therefore $P \in \Pi'$. Conversely, if $P \in \Pi'$, then $P \supseteq P_0 \supseteq I_p(\Pi) \cap F$, where $P_0 \in \Pi_0$. Consequently, $P = P \cdot J \supseteq (I_p(\Pi) \cap F) \cdot J = I_p(\Pi)$. Thus, $P \in \Pi$. This shows that $J_\Pi = J_{\Pi'}$, so by Proposition 2.9, F is a field of definition of J_Π.

Corollary 2.11. *If Π is a set of prime ideals of J, then the following conditions are equivalent:*

(i) *If F is a proper subfield of K, there is a rational prime p such that $I_p(\Pi)$ is* not *generated by the elements of F;*

(ii) *K is the smallest field of definition of J_Π;*

(iii) *As a group, J_Π is strongly indecomposable (that is, J_Π is not quasi-equal to any proper direct sum).*

Proof. The conditions (i) and (ii) are equivalent by Theorem 2.10. The equivalence of (ii) and (iii) was proved in [5].

Corollary 2.12. *Let Π be a set of prime ideals of J such that for some rational prime p, there is precisely one $P \in \Pi$ with $p \in P$, and such that this prime ideal is unramified and has degree one. Then K is the smallest field of definition of J_Π.*

Proof. Le F be a field of definition of J_Π. Then by Theorem 2.10, $P = (P \cap F) \cdot J$. Thus $[K:F] =$ degree of $P = 1$ (see [6, p. 287]). Consequently, K is the smallest field of definition of J_Π.

This corollary provides a method of constructing full subrings of K whose smallest field of definition is K. Indeed, if $\Pi = \{P\}$ where P is unramified of degree one (and such prime ideals exist in abundance), then J_Π is such a ring.

3. The quasi-isomorphism classes. Our objective in this section is to survey all full subrings belonging to a fixed quasi-isomorphism class. By the results of Section 2, this is equivalent to the problem of classifying the subrings of finite index in a ring J_Π. A fairly obvious method of constructing subrings of finite index in J_Π is to take the preimage in J_Π of subrings of finite rings J_Π/I, where I is a non-zero ideal of J_Π. It is evident that every subring of finite index in J_Π can be obtained in this way. Unfortunately, the same ring may be captured many times, using different ideals of J_Π. In order to secure uniqueness, one is led to examine the subrings of finite index in the inverse limit of the system of rings $\{J_\Pi/I\}$ (defined in the obvious way). It is then natural to look at the structure of this inverse limit. It turns out to be a complete direct sum of the rings $J(P)$, $P \in \Pi$. However, the proof of this fact is somewhat intricate. It is easier to relate directly the subrings of finite index in J_Π to the subrings of finite index in this complete direct sum. The main purpose of the present section is to establish this correspondence.

If Π is any set of prime ideals of J, define

$$J(\Pi) = \sum_{P \in \Pi}^{*} J(P),$$

the complete direct sum with the cartesian product topology. The elements

of $J(\Pi)$ will be denoted $[\xi_P]$. Since $J_\Pi \subseteq J_P$ for all $P \in \Pi$, there is a uniquely defined injection

$$\Delta : J_\Pi \to J(\Pi),$$

obtained by letting $\Delta(x) = [\Delta_P x]$. For any non-zero ideal I of J, define

$$V(I) = \{[\xi_P] \in J(\Pi) \mid v_P(\xi_P) \leqq v_P(I) \quad \text{for all} \quad P \in \Pi\}.$$

Lemma 3.1. (i) *$J(\Pi)$ is a compact topological ring.* (ii) *The sets $V(I)$ are open and constitute a complete system of neighborhoods of zero in $J(\Pi)$.* (iii) *$\Delta(J)$ is dense in $J(\Pi)$.*

Proof. Of these assertions, only the last requires comment. Let $[\xi_P] \in J(\Pi)$ and let I be a non-zero ideal of J. Since $\Delta_P(J)$ is dense in $J(P)$, there exist $x_P \in J$ such that $v_P(\Delta_P(x_P) - \xi_P) \leqq v_P(I)$ for all $P \in \Pi$. By the generalized Chinese remainder theorem, there is an $x \in J$ such that $v_P(x - x_P) \leqq v_P(I)$ for all $P \in \Pi$ satisfying $v_P(I) < 1$. Consequently, $\Delta(x) - [\xi_P] \in V(I)$. By (ii) it follows that $\Delta(J)$ is dense in $J(\Pi)$.

Lemma 3.2. *If I_1 and I_2 are non-zero ideals of J with $I_1 \subseteq I_2$, then $V(I_1) \subseteq V(I_2) \subseteq \Delta(I_2) + V(I_1)$.*

Proof. If $I_1 \subseteq I_2$, then $v_P(I_1) \leqq v_P(I_2)$ for all P, so that $V(I_1) \subseteq V(I_2)$. Suppose $[\xi_P] \in V(I_2)$. By Lemma 3.1, there exists $x \in J$ such that $\Delta(x) - [\xi_P] \in V(I_1)$. But then $v_P(x) \leqq v_P(I_2)$ for all $P \in \Pi$. By the generalized Chinese remainder theorem, there is an element $y \in J$ such that $v_P(x - y) \leqq v_P(I_1)$ for all $P \in \Pi$ with $v_P(I_1) < 1$, and $v_P(y) \leqq v_P(I_2)$ for all $P \in \Pi^*$ with $v_P(I_2) < 1$. It follows that $\Delta(y) - [\xi_P] \in V(I_1)$ and that $v_P(y) \leqq v_P(I_2)$ for all P. Hence, $y \in I_2$ and $[\xi_P] \in \Delta(I_2) + V(I_1)$.

Lemma 3.3. *Let A be a subgroup of J_Π which contains the ideal I_0 of J. Then the closure of $\Delta(A)$ in $J(\Pi)$ is $\Delta(A) + V(I_0)$.*

Proof. As in any commutative topological group, the closure of $\Delta(A)$ is the intersection $\bigcap_N (\Delta(A) + N)$, where N ranges over any complete system of neighborhoods of zero. Thus, by Lemmas 3.1 and 3.2 this closure is $\bigcap_{I \subseteq I_0} (\Delta(A) + V(I)) = \Delta(A) + V(I_0)$. Indeed, $\Delta(A) + V(I) = \Delta(A) + \Delta(I_0) + V(I) \supseteq \supseteq \Delta(A) + V(I_0)$ for $I \subseteq I_0$.

Lemma 3.4. *If I is a non-zero ideal of J, then $\Delta^{-1}(V(I)) = IJ_\Pi$.*

Proof. By definition, $u \in \Delta^{-1}(V(I))$ if and only if $v_P(u) \leqq v_P(I)$ for all $P \in \Pi$. By definition of v_P, this implies that $(u) = uJ = II'(I'')^{-1}$, where I' and I'' are (integral) ideals and I'' is a product to prime ideals which are not in Π. Thus, $z \in (I'')^{-1}$ implies $zI'' \subseteq J$ and therefore $v_P(z) \leqq 1$ for all P

not dividing I''. In particular, $v_P(z) \leqq 1$ for all $P \in \Pi$. Thus, $z \in J_\Pi$. It follows that $I'(I'')^{-1} \subseteq J_\Pi$ and therefore $u \in IJ_\Pi$. Conversely, if $u = x_1w_1 + \cdots + x_kw_k$, $x_i \in I$, $w_i \in J_\Pi$, then for any $P \in \Pi$,

$$v_P(u) \leqq \max\{v_P(x_1)v_P(w_1), \ldots, v_P(x_k)v_P(w_k)\} \leqq v_P(I).$$

Hence, $u \in \Delta^{-1}(V(I))$.

Lemma 3.5. *The following conditions are equivalent for subgroups L of $J(\Pi)$:*

(i) *L has finite index in $J(\Pi)$;*
(ii) *$J(\Pi)/L$ has bounded order;*
(iii) *$V(I) \subseteq L$ for some non-zero ideal I of J;*
(iv) *L is open.*

Proof. Clearly (i) implies (ii). Property (ii) implies property (iii), since if n is a non-zero integer such that $nJ(\Pi) \subseteq L$, then $V((n)) = nJ(\Pi) \subseteq L$. If (iii) is satisfied, then $L = \cup\{x + V(I) | x \in L\}$ is a union of open sets, hence open. Finally (iv) implies (i) since $J(\Pi)$ is a disjoint union of the cosets of L and by the compactness of $J(\Pi)$, this union must be finite.

For $A \subseteq J_\Pi$, let $\Delta(A)^-$ denote the closure of $\Delta(A)$ in $J(\Pi)$.

Theorem 3.6. *The mappings*

$$A \to \Delta(A)^-, \quad L \to \Delta^{-1}(L)$$

are inverse, one-to-one correspondences between the subgroups A of finite index in J_Π and the open subgroups L of $J(\Pi)$. These correspondences send subrings into subrings, subrings with identity into subrings with identity, and ideals into ideals.

Proof. If A has finite index in J_Π, then A contains a non-zero ideal of J and therefore by Lemmas 3.3 and 3.5, $\Delta(A)^-$ is an open subgroup of $J(\Pi)$. Let I be a non-zero ideal of J such that $IJ_\Pi \subseteq A$. (For example, if $nJ_\Pi \subseteq A$, let $I = (n)$.) Necessarily $I \subseteq A$. Thus, by Lemmas 3.3 and 3.4, $\Delta^{-1}(\Delta(A)^-) = \Delta^{-1}(\Delta(A) + V(I)) = A + \Delta^{-1}(V(I)) = A + IJ_\Pi = A$. By Lemma 3.5, if L is an open subgroup of $J(\Pi)$, there is a non-zero ideal I in J such that $V(I) \subseteq L$. Consequently, by Lemma 3.4, $\Delta^{-1}(L) \supseteq IJ_\Pi \supseteq nJ_\Pi$, where n is any non-zero integer in I. It follows that $\Delta^{-1}(L)$ has finite index in J_Π. To prove that $\Delta(\Delta^{-1}(L))^- = L$, we have only to note that L is an open and therefore closed subgroup of $J(\Pi)$, that $\Delta(\Delta^{-1}(L)) = \Delta(J_\Pi) \cap L$, and finally that $\Delta(J_\Pi)$ is dense in $J(\Pi)$ (by Lemma 3.1). The last statements of the theorem are consequences of the facts that the closure of a subring of a topological ring is itself a subring, and that the closure of an ideal of a dense subring is an ideal of the ring.

By virtue of Theorem 3.6, the problem of finding subrings of finite index in a ring is transferred from J_Π to $J(\Pi)$. In many respects, this is a simplification. For example, one has the following result.

Proposition 3.7. *Let L be an open subgroup in $J(\Pi)$. Then $L=\sum_p^* L^p$, where $L^p=L\cap\left(\sum_{p\in P\in\Pi} J(P)\right)$ and $L^p=\sum_{p\in P\in\Pi} J(P)$ for almost all p.*

Proof. By Lemma 3.5, $L\supseteq V((n))$, where n is some non-zero rational integer. Let $\Pi'=\{P\in\Pi\mid n\notin P\}$. Then $\Pi-\Pi'$ is finite and, by definition, $V((n))$ contains $J(\Pi')=\sum_{p\in\Pi'}^* J(P)$. In particular, $V((n))$ contains the identity e of $J(\Pi')$. Hence $eV((n))\subseteq eL\subseteq eJ(\Pi)=eV((n))$. Thus

$$L=(1-e)L\oplus eL=(1-e)L\oplus\sum_{p\in\Pi'}^* J(P)=(1-e)L+\sum_{(p,n)=1}^* L^p,$$

since $(p,n)=1$ implies $L\cap\sum_{p\in P\in\Pi} J(P)=V((n))\cap\sum_{p\in P\in\Pi} J(P)=\sum_{p\in P\in\Pi} J(P)$. Now let $n=p^k n'$, where $(p,n')=1$. Then

$$n'(1-e)L=L\cap\left(\sum_{p\in P\in\Pi} J(P)\right)+(1-e)V((n)).$$

Hence, $(1-e)L=\sum_{p\mid n}(L\cap\sum_{p\in P\in\Pi} J(P))+(1-e)V((n))=\sum_{p\mid n} L^p$, and this last sum is direct. Therefore, finally $L=\sum_p^* L^p$.

As an application of these results, we will "count" the subrings of finite index in J_Π which contain the identity element of K. It turns out that J_Π either has no proper subrings containing 1, or it has infinitely many such subrings. To prove this fact, it suffices by Proposition 3.7 to examine the subrings of $J(\Pi_p)$, where $\Pi_p=\{P\in\Pi\mid p\in P\}$.

Lemma 3.8. *Let A be a torsion free group such that A/pA has rank at least two. Let x be any element of A. Define $B_k=\{x,p^kA\}$. Then $A=B_0\supset B_1\supset B_2\supset\cdots$.*

Proof. Clearly $A=B_0\supseteq B_1\supseteq B_2\supseteq\cdots$. We must prove that the inclusions are strict. Since A is torsion free, the mapping $p\colon p^{k-1}A\to p^kA$ is an isomorphism which sends p^kA onto $p^{k+1}A$. Hence $p^kA/p^{k+1}A\cong A/pA$ has rank at least two. From the exactness of the sequence

$$0\to(p^kA\cap\{x\})/(p^{k+1}A\cap\{x\})\to p^kA/p^{k+1}A\to B_k/B_{k+1}\to 0,$$

it follows that $B_{k+1}\subset B_k$.

Corollary 3.9. *Let p be a rational prime. Then the ring $J(\Pi_p)=\sum_{p\in P\in\Pi} J(P)$ contains infinitely many distinct open subrings with identity un-*

less either $\Pi_p = \emptyset$, *or* $\Pi_p = \{P\}$, *where* P *is unramified over* p *and the degree of* P *is one.*

Proof. Let $A = J(\Pi_p)$. We can assume that $A \neq 0$. If Π_p contains more than one prime ideal, than A/pA has rank at least two, because p is not a unit of $J(P)$ if $p \in P$. Suppose that $A = J(P)$. If P is ramified over p, then A/pA is an algebra (over Z_p) whose radical is neither zero nor the whole algebra. Thus again A/pA has rank larger than one. Finally, if P is unramified, then $A/pA \cong J/P$ has rank equal to the degree of P. Therefore, unless $\Pi_p = \{P\}$ where P is unramified of degree one, Lemma 3. 8 is applicable and by taking x to be the identity element 1 of K, the corresponding subgroups B_k are actually subrings containing 1. These are open by Lemma 3. 5.

Lemma 3. 10. *Let* P *be an unramified prime ideal in* J *which is of degree one. Then the open subgroups of* $J(P)$ *are precisely those of the form* $p^n J(P)$, $n \geqq 0$, *where* p *is the rational prime belonging to* P. *In particular, there is no proper open subgroup of* $J(P)$ *containing* 1.

Proof. Since P is unramified and of degree one, $J(P)/pJ(P) \cong J/P \cong Z_p$ (the integers modulo p). Thus, for any k, $J(P)/p^k J(P)$ is a cyclic group of order p^k. Suppose L is an open subgroup of $J(P)$. Then by Lemma 3. 5, $L \supseteq p^k J(P)$ for some k. Consequently $L/p^k J(P)$ is a subgroup of $J(P)/p^k J(P)$. Since $J(P)/p^k J(P)$ is cyclic of order p^k, there is an integer $n \leqq k$ such that $L/p^k J(P) = p^n(J(P)/p^k J(P))$. Thus, $L = p^n J(P)$.

For convenience, we will say that the set Π of prime ideals of J *satisfies condition* U if

(i) for any rational prime p, $\Pi_p = \{P \in \Pi \mid p \in P\}$ contains at most one prime ideal, and

(ii) if $P \in \Pi$, then P is unramified and of degree one.

Theorem 3. 11. *Let* Π *be a set of prime ideals of* J. *If* Π *satisfies condition* U, *then every subgroup of finite index in* J_Π *is of the form* nJ_Π, *where* n *is a rational integer. In particular, every ideal of* J_Π *is generated by a rational integer. Moreover, there is no proper subring of finite index in* J_Π *which contains the identity element. If* Π *fails to satisfy condition* U, *then there is a countable infinity of proper subrings of finite index in* J_Π, *each of which contains the identity.*

Proof. Suppose that Π satisfies condition U. Then by Proposition 3. 7 and Lemma 3. 10, every open subgroup L of $J(\Pi)$ is of the form $\sum_p{}^* L^p$, where $L^p = 0$ if $\Pi_p = \emptyset$ and $L^p = p^{k(p)} J(P)$ if $\Pi_p = \{P\}$ with $k(p) = 0$ for almost all such p. Moreover if $1 \in L$, then $k(p) = 0$ for every prime p such that $\Pi_p \neq \emptyset$. Let n be the product of all $p^{k(p)}$. Then $L = nJ(\Pi)$. We con-

clude from Theorem 3.6 that each subgroup of finite index in J_Π is of the form nJ_Π, with $n=1$ for subgroups containing the identity of K. If Π does not satisfy condition U, then by Corollary 3.9, Proposition 3.7 and Theorem 3.6, J_Π contains infinitely many subrings of finite index, each of which contains the identity. Since J_Π/mJ_Π is finite for any non-zero integer m, there can be at most a countable number of subrings (or even subgroups) of finite index in J_Π.

Corollary 3.12. *Let Π be a set of prime ideals of J such that K is the smallest field of definition of J_Π* (see Corollary 2.11). *Suppose that Π does not satisfy condition U. Then the quasi-equality class of J_Π contains infinitely many rings with identity no two of which are group isomorphic.*

Proof. It is sufficient to show that if A and B are full subrings of J_Π containing the identity, and if A and B are group isomorphic, then $A=B$. Let φ be an isomorphism of A onto B. By the results of [5], there is a non-zero element $z\in K$ such that $\varphi(x)=z\cdot x$ for all $x\in A$. Thus $z=z\cdot 1=\varphi(1)\in B$. Since B is a ring, $z^2\in B$. Since φ is onto, there is an $x\in A$ such that $z^2=\varphi(x)=zx$, that is $z\in A$. Therefore, $B=zA\subseteq A$. By symmetry, $A=B$.

If K is not the smallest field of definition of J_Π, then Π cannot satisfy condition U unless $\Pi=\emptyset$ (by Corollary 2.12). However, Π can satisfy condition U relative to the smallest field of definition of J_Π, in the sense of the following result.

Corollary 3.13. *Suppose that F is the smallest field of definition of J_Π and that $\Pi_0=\{P\cap F\mid P\in\Pi\}$ satisfies condition U (relative to the ring of integers in F). Let A be a subring of K such that $A\doteq J_\Pi$. Then A is group isomorphic to the direct sum $B_1\oplus\cdots\oplus B_k$, where $B_i\cong J_{\Pi_0}\cong A\cap F$ and $k=[K:F]$.*

Proof. Let $C=\{x\in F\mid xA\subseteq A\}$. Then $1\in C$ and $A\cap F\subseteq C$. If $n\neq 0$ is such that $n\cdot 1\in A$, then $nx=x(n\cdot 1)\in A$ for every $x\in C$. Thus, $nC\subseteq A\cap F$. Consequently, C is a full subring of F which belongs to the quasi-equality class of $A\cap F$. By theorem 2.10, this is the same as the quasi-equality class of J_{Π_0}. Thus by Theorem 3.11 and the assumption that Π_0 satisfies condition U, we conclude that $C=J_{\Pi_0}$. In particular, C is a principal ideal domain. Since F is a field of definition of A, there is a basis $\{x_1,\ldots,x_k\}$ of K over F such that $A\doteq(A\cap F)x_1+\cdots+(A\cap F)x_k\doteq Cx_1+\cdots+Cx_k$. Thus if m is a non-zero integer such that $mx_i\in A$ for $i=1,\ldots,k$, then $A/(C(mx_1)+\cdots+C(mx_k))$ is a group of finite rank and bounded order — hence finite. Consequently, A is a finitely generated C-module. From the structure theory of modules over a principal ideal domain (see [6, p. 247]), we conclude that there is a basis $\{y_1,\ldots,y_k\}$ of K over F such that $A=Cy_1+\cdots+Cy_k$. By

Theorem 3.11, $C = J_{\Pi_0} \cong A \cap F$ (as groups). This completes the proof, but we remark that if $1 \in A$, then $A \cap F = J_{\Pi_0}$ and A is a free $A \cap F$-module.

If the smallest field of definition of J_Π is Q, then Π_0 is a set of rational primes (or the principal ideals which they generate) and Π_0 automatically satisfies condition U. Thus any full subring of K whose smallest field of definition is Q is group isomorphic to a direct sum of copies of a rank one group. This fact was proved in [1] by a different method.

4. Additive groups of subrings of algebraic number fields. A torsion free group A is called a *quotient divisible group* (or q. d. group) if A contains a full free subgroup F such that A/F is divisible. This concept was introduced in [1], where it was shown that the additive group of a full subring of a semi-simple rational algebra (finite dimensional) is always a q. d. group. This result provides a necessary condition on a torsion free group in order that it be isomorphic to the additive group of a subring of an algebraic number field. Another necessary condition is obtained from the following theorem which is proved in [5]. Let $E(A)$ denote the ring of endomorphisms of the group A. If A is (the additive group of) a full subring of the algebraic number field K, then $Q \otimes E(A)$ is isomorphic (as a rational algebra) to the full matrix ring $M_m(F)$, where F is the smallest field of definition of A and $m = [K:F]$.

For a torsion free group A, the rational algebra $Q \otimes E(A)$ is an invariant of considerable interest. On the one hand, $Q \otimes E(A)$ usually has simpler structure than A. On the other hand, $Q \otimes E(A)$ reflects many interesting properties of A. It is often possible to determine $Q \otimes E(A)$ explicitly. For example, if A is a rank one group, then $Q \otimes E(A)$ is always isomorphic to Q. For rank two groups, the algebras $Q \otimes E(A)$ have also been calculated (see [2]). Finally, as we noted above, the algebras $Q \otimes E(A)$ are known if A is the additive group of a full subring of an algebraic number field (or more generally, a simple Q-algebra).

If A is a full subgroup of the rational vector space V, it is possible to identify $Q \otimes E(A)$ with a subalgebra of the ring $E(V)$ of all linear transformations of V, namely

$$QE(A) = \{\varphi \in E(V) \mid n\varphi(A) \subseteq A \quad \text{for some} \quad n \neq 0\}.$$

Notationally, $QE(A)$ is easier to work with than $Q \otimes E(A)$.

The purpose of this section is to prove the following:

Theorem 4.1. *Let A be a torsion free group of rank n. Let K be an algebraic number field. Then A is isomorphic to the additive group of a full subring of K if and only if $[K:Q] = n$, A is a q. d. group, and $Q \otimes E(A)$ is isomorphic to $M_m(F)$ where F is a subfield of K such that $[K:F] = m$.*

The condition $[K:Q]=n$ is clearly necessary and the necessity of the other conditions has been established in the papers mentioned above. The proof that these conditions are sufficient will be accomplished in several steps. We may assume throughout that A is a full q. d. subgroup of the n dimensional rational space V and that $QE(A)\cong M_m(F)$, where F is a subfield of K such that $[K:F]=m$.

(4. 2) If $A\doteq B$ and B is isomorphic to a full subring of K, then A is isomorphic to a full subring of K.

This was proved in [1, Corollary 2. 7].

(4. 3) It suffices to prove the theorem in the case $m=1$.

Suppose that the theorem is true for $m=1$. Let φ_{ij} denote the mappings corresponding to the matrix units under the isomorphism $QE(A)\cong M_m(F)$. In particular, the set $\{\varphi_{11},\ldots,\varphi_{mm}\}$ is a family of orthogonal projections whose sum is the identity map. Moreover $\varphi_{ii}QE(A)\varphi_{ii}\cong F$. Let $A_i=\varphi_{ii}(A)$. Since $\varphi_{ij}\in QE(A)$, there is an integer $k\neq 0$ such that $k\varphi_{ij}(A)\subseteq A$ for all i and j. Then $kA_i=k\varphi_{ii}(A)=\varphi_{ij}(k\varphi_{ji}(A))\subseteq\varphi_{ij}(A)$ and $k\varphi_{ij}(A)=\varphi_{ii}(k\varphi_{ij}(A))\subseteq$ $\subseteq\varphi_{ii}(A)=A_i$. Since φ_{ij} maps A_j isomorphically onto $\varphi_{ij}(A)$, we therefore have $A_i\doteq\varphi_{ij}(A)\cong A_j$. Moreover $k(A_1+\cdots+A_m)\subseteq A=(\varphi_{11}+\cdots+\varphi_{mm})A\subseteq$ $\subseteq A_1+\cdots+A_m$, so that $A\doteq A_1\oplus\cdots\oplus A_m$. Now the hypotheses of Theorem 4. 1 are satisfied for the case $m=1$, since rank $A_i=(1/m)$ rank $A=$ $=[K:Q]/[K:F]=[F:Q]$, each A_i is a q. d. group ([1, Corollary 5. 8], and $QE(A_i)\cong\varphi_{ii}QE(A)\varphi_{ii}\cong F$. Hence $A_i\cong B_i$ where B_i is a full subring of F, and $B_1\doteq\cdots\doteq B_m$. Let $B=B_1\cap\cdots\cap B_m$. Then K contains a full subring C which is group isomorphic to a direct sum of m copies of B. Thus, C is isomorphic to a subgroup of finite index in $A_1\oplus\cdots\oplus A_m$. Consequently, by (4. 2) A is isomorphic to a full subring of K.

We suppose henceforth that $m=1$, that is, $QE(A)\cong K$. Choose any $a\neq 0$ in A and define $\theta: QE(A)\to V$ by $\theta(\varphi)=\varphi(a)$. Clearly, θ is a Q-space homomorphism. Since $QE(A)$ is a field and the kernel of θ is an ideal (and θ is not the zero map), it follows that θ is one-to-one. Since both $QE(A)$ and V have dimension equal to n, the mapping θ is onto. Therefore θ induces a multiplication on V satisfying $\theta(\varphi)\theta(\psi)=\theta(\varphi\psi)$. That is, with respect to this multiplication, θ is a ring isomorphism of $QE(A)$ on V. Hence V is a ring which is isomorphic to K. Note that for any $x\in V$ and $\varphi\in QE(A)$,

(4. 4) $\varphi(a)\cdot x=\varphi(x)$.

Indeed, we can write $x=\theta(\psi)$ for some $\psi\in QE(A)$, and $\varphi(a)\cdot x=\theta(\varphi)\theta(\psi)=$ $=\theta(\varphi\psi)=\varphi(\psi(a))=\varphi(x)$.

(4. 5) A is quasi-equal to a subring of V.

This result, together with (4. 2), will complete the proof of Theorem 4. 1. The proof of (4. 5) is based on a criterion established in [1] (Theorem 1. 10): a q. d. subgroup A of the finite dimensional rational algebra V is quasi-equal to a subring of V if, for each prime p, the $Q(p)$-space

$$\delta_p(A) = d(Z(p) \otimes A)$$

(the maximal divisible subgroup of $Z(p) \otimes A$, considered as a subgroup of $Q(p) \otimes V$) is an ideal of $Q(p) \otimes V$.

Suppose $z \in V$. Write $z = \varphi(a)$, $\varphi \in QE(A)$. If $w \in Q(p) \otimes V$, say $w = \Sigma \alpha_i \otimes x_i$ $(\alpha_i \in Q(p),\ x_i \in V)$, then by (4. 4), $(1 \otimes z)w = \Sigma \alpha_i \otimes z x_i = \Sigma \alpha_i \otimes \varphi(x_i) = (1 \otimes \varphi)w$. In particular, $(1 \otimes z)\delta_p(A) = (1 \otimes \varphi)\delta_p(A)$. If $z \neq 0$, then φ is a non-singular transformation of V and in this case it is clear that $(1 \otimes \varphi)\delta_p(A) = \delta_p(\varphi A)$. Moreover, $k\varphi(A) \subseteq A$ for some non-zero integer k since $\varphi \in QE(A)$. Thus, $\delta_p(\varphi A) = k\delta_p(\varphi A) = \delta_p(k\varphi(A)) \subseteq \delta_p(A)$. Combining these observations gives $(1 \otimes z)\delta_p(A) \subseteq \delta_p(A)$ for all $z \neq 0$ in V. Since the elements of the form $1 \otimes z$ span $Q(p) \otimes V$ over $Q(p)$, and since $\delta_p(A)$ is a $Q(p)$-subspace of $Q(p) \otimes V$, it follows that $\delta_p(A)$ is an ideal of $Q(p) \otimes V$. This is the result which was needed to complete the proof of (4. 5).

Corollary 4.6. *Let A be a torsion free group of finite rank. Then A is isomorphic to the additive group of a full subring of a semi-simple rational algebra if and only if A is a q. d. group and A is quasi-equal to a direct sum $B_1 \oplus \cdots \oplus B_r$ of strongly indecomposable groups such that each of the rings $Q \otimes E(B_i)$ is an algebraic number field whose dimension over Q is the rank of B_i.*

Proof. Suppose first that A satisfies these conditions. Then each B_i is a q. d. group (by [1, Corollary 5. 8]) and therefore by Theorem 4. 1 each B_i is isomorphic to the additive group of a full subring of an algebraic number field. It follows, using (4. 2), that A is isomorphic to a full subring of a direct sum of fields. The necessity of these conditions is obtained from the results of [1] and [5].

References

[1] R. A. Beaumont and R. S. Pierce, Torsion-free rings, *Illinois J. Math.*, **5** (1961), 61—98.
[2] R. A. Beaumont and R. S. Pierce, Torsion free groups of rank two, *Memoirs Amer. Math. Soc.*, **38** (1961).
[3] M. Deuring, *Algebren* (Berlin, 1935).
[4] W. Krull, *Idealtheorie* (Berlin, 1935).
[5] R. S. Pierce, Subrings of simple algebras, *Michigan Math. J.*, 7 (1960), 241—243.
[6] O. Zariski and P. Samuel, *Commutative Algebra*, vol. 1, (Princeton, 1958).

UNIVERSITY OF WASHINGTON

(Received October 11, 1960)